

**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING
UNDER 35 U.S.C. 371**

U.S. APPLICATION NO.
(If known, see 37 CFR 1.5)
10/049591

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/06176	23 August 1999	23 August 1999

TITLE OF INVENTION	Sending Initial Password Through an SMS
--------------------	--

APPLICANT(S) FOR DO/EO/US	Michael T. ANDERSEN
---------------------------	----------------------------

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

- [x] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
- [] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371
- [x] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [x] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
- [x] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
- a. [x] is transmitted herewith (required only if not transmitted by the International Bureau).
- b. [x] has been transmitted by the International Bureau
- c. [] is not required, as the application was filed in the United States Receiving Office (RO/US)
- [] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [x] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
- a. [x] are transmitted herewith (required only if not transmitted by the International Bureau). (**See Reply to Written Opinion**)
- b. [] have been transmitted by the International Bureau.
- c. [] have not been made; however, the time limit for making such amendments has NOT expired.
- d. [] have not been made and will not be made.
8. [] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [x] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). **Unexecuted**
10. [] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5))

Items 11. to 16. Below concern other document(s) or information included:

11. [x] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [x] A **FIRST** preliminary amendment.
- [] A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. [] A substitute specification.
15. [] A change of power of attorney and/or address letter
16. [x] Other items or information (*specify*) PCT Publication Sheet, Int'l Preliminary Examination Report, Written Opinion, Reply to Written Opinion, PCT Request, Information Concerning Elected Offices Notified of their Election, Notice Informing the Applicant of the Communication of the International Application to the Designated Offices, Notification of the Recording of a Change, Notification of Receipt of Record Copy

10/049591

PCT/EP99/06176

4925-206PUS

17.[x] The following fees are submitted:

Basic National Fee (37 CFR 1.492(a)(1)-(5)):

Search Report has been prepared by the LPO or IPO	\$890.00
International preliminary examination fee paid to USPTO (37 CFR 1.482)	\$710.00
No international preliminary examination fee paid to USPTO (37 CFR 1.482)	
but international search fee paid to USPTO (37 CFR 1.445(a)(2)).....	\$740.00
Neither international preliminary examination fee (37 CFR 1.482)	
nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO	\$1040.00
International preliminary examination fee paid to USPTO (37 CFR 1.482)	
and all claims satisfied provisions of PCT Article 33(2)-(4)	\$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =	\$ 890
--------------------------------------	--------

Surcharge of \$130.00 for furnishing the oath or declaration later than [] 20 [] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	\$
---	----

Claims	Number Filed	Number Extra	Rate	
Total Claims	21 - 20 =	1	x \$18.00	\$ 18
Independent Claims	2 - 3 =		x \$84.00	\$
Multiple dependent claim(s) (if applicable)			+ \$280.00	\$
				TOTAL OF ABOVE CALCULATIONS = \$ 908
Reduction of ½ for filing by small entity, if applicable.				\$
				SUBTOTAL = \$ 908
Processing fee of \$130.00 for furnishing the English translation later than [] 20 [] 30 months from the earliest claimed priority date (37 CFR 1.492(f)).			+ \$	
				TOTAL NATIONAL FEE = \$ 908
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by the appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property			+ \$	
				TOTAL FEES ENCLOSED \$ 908
				Amount to be refunded: \$
				charged: \$

- a. [x] One check in the amount of \$908 to cover the above fee is enclosed.
- b. [] Please charge my Deposit Account No. 03-2412 in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. [x] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No 03-2412. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

Michael C. Stuart

Cohen, Pontani, Lieberman & Pavane
551 Fifth Avenue, Suite 1210
New York, New York 10176

Form PTO-1390 (REV 10-94)

Michael C. Stuart

Registration Number: 35,698 February 13, 2002

Tel. (212) 687-2770

By Express Mail # EV052763547US · February 13, 2002

Attorney Docket # 4925-206PUS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re National Phase PCT Application of

Michael T. ANDERSEN

International Appln. No.: PCT/EP99/06176

International Filing Date: 23 August 1999

For: Sending Initial Password Through an SMS

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

BOX PCT

SIR:

Prior to examination of the above-identified application please amend the application as follows:

IN THE SPECIFICATION:

Page 4, delete lines 16 and 17, and substitute therefor the following paragraph:

-- Other objects and features of the present invention will become apparent from the following detailed description considered in conjunction with the accompanying drawings. It is to be understood, however, that the drawings are intended solely for purposes of illustration and not as a definition of the limits of the invention, for which reference should be made to the appended claims.--

Page 5, replace the paragraph beginning on line 14 with the following rewritten paragraph:

--The MSC 3 comprises a Service Switching Point (SSP) 31 which implements a service switching function and which also provides an interface between a Services Control Point (SCP) 4 and the MSC 3. The SCP 4 serves to control the services requests etc. and is the function in the telecommunications network, which has access to data and logic for controlling processing of a call in order to provide a supplementary service. The SCP 4 is connected with a service management point (SMP) 5 in which IN services offered in the corresponding Intelligent Network are managed. In particular, also subscriber data such as an MSISDN (Mobile Station ISDN Number, i.e., Mobile Station Integrated Services Digital Network Number) are stored in the SMP 5.--

Page 10, delete lines 17 to 20 and substitute therefor following paragraph:

--Thus, while there have been shown and described and pointed out fundamental novel features of the present invention as applied to preferred embodiments thereof, it will be understood that various omissions and substitutions and changes in the form and details of the devices described and illustrated, and in their operation, and of the methods described may be made by those skilled in the art without departing from the spirit of the present invention. For example, it is expressly intended that all combinations of those elements and/or method steps which perform substantially the same function in substantially the same way to achieve the same results are within the scope of the invention. Substitutions of elements from one described embodiment to another are also fully intended and contemplated. It is the intention, therefore, to be limited only as indicated by the scope of the claims appended hereto.--.

Page 11, line 2, delete "Claims" and substitute therefor --What is claimed is:--.

IN THE CLAIMS:

Claims 3, 6, 9 and 12 have been amended to read as follows:

3. The services management method according to claim 1, wherein said access code comprises a subscriber identification number.

6. The services management method according to claim 1, further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

9. The services management method according to claim 7, wherein said access code comprises a subscriber identification number.

12. A subscriber terminal which is adapted to receive data messages transmitted by a services management device according to claim 8, further comprising a detecting means (11) for detecting said access code.

Add the following new claims:

13. The services management method according to claim 2, wherein said access code comprises a subscriber identification number.

14. The services management method according to claim 2, further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

15. The services management method according to claim 3, further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

16. The services management method according to claim 4, further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

17. The services management method according to claim 5, further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

18. The services management method according to claim 8, wherein said access code comprises a subscriber identification number.

19. A subscriber terminal which is adapted to receive data messages transmitted by a services management device according to claim 9, further comprising a detecting means (11) for detecting said access code.

20. A subscriber terminal which is adapted to receive data messages transmitted by a services management device according to claim 10, further comprising a detecting means (11) for detecting said access code.

21. A subscriber terminal which is adapted to receive data messages transmitted by a services management device according to claim 11, further comprising a detecting means (11) for detecting said access code.

REMARKS

This preliminary amendment is presented to place the application in proper form for examination and to eliminate multiple dependency from the present claims. No new matter has been added. Early examination and favorable consideration of the above-identified application is earnestly solicited.

Attached hereto is a mark-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "Version with markings to show changes made".

Any additional fees or charges required at this time in connection with the application may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN, PONTANI, LIEBERMAN & PAVANE

By:



Michael C. Stuart
Reg. No. 35,698
551 Fifth Avenue, Suite 1210
New York, N.Y. 10176
(212) 687-2770

13 February 2002

AMENDMENTS TO THE SPECIFICATION AND CLAIMS SHOWING CHANGES

The specification has been amended as follows:

Page 5, the paragraph beginning on line 14 has been amended as follows:

--The MSC 3 comprises a Service Switching Point (SSP) 31 which implements a service switching function and which also provides an interface between a Services Control Point (SCP) 4 and the MSC 3. The SCP 4 serves to control the services requests etc. and is the function in the telecommunications network, which has access to data and logic for controlling processing of a call in order to provide a supplementary service. The SCP 4 is connected with a service management point (SMP) 5 in which IN services offered in the corresponding Intelligent Network are managed. In particular, also subscriber data such as an MSISDN (Mobile Station ISDN Number, i.e., Mobile Station [station] Integrated Services Digital Network Number) are stored in the SMP 5 [54].--

By Express Mail # EV052763547US · February 13, 2002

In the Claims:

3. The services management method according to claim 1 [or 2], wherein said access code comprises a subscriber identification number.

6. The services management method according to claim 1 [any one of the previous claims], further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

9. The services management method according to claim 7 [or 8], wherein said access code comprises a subscriber identification number.

12. A subscriber terminal which is adapted to receive data messages transmitted by a services management device according to claim 8 [any one of the claims 8 to 11], further comprising a detecting means (11) for detecting said access code.

SENDING INITIAL PASSWORD THROUGH AN SMSField of the invention

5

The present invention relates to a services management method for managing subscriber services and to a corresponding device, which serve in particular to supply a subscriber of services of a network with a password.

10

BACKGROUND OF THE INVENTION

There are a plurality of networks which offer special services for subscribers. An example for such networks is the so-called Intelligent Network (IN). The term Intelligent Network describes a network, in which new services can easily be introduced without the need to replace or upgrade switches or network control devices, 20 including those under customer control.

In such an Intelligent Network, a subscriber or service provider can manage his own services by a network user interface. This management is handled by a so called 25 Service Management Access Point (SMAP).

SMAP is an access system which provides the customers and service providers an open interface to different telecommunication network elements. They can update by 30 using SMAP their service data in a secure and controlled manner on self-service basis in an intelligent network or other telecommunication network. A more detailed description of SMAP can be found in Nokia's patent application WO 98/41038.

35

- 2 -

In general, the communications between the subscriber and the SMAP have been handled so far by an Interactive Voice Prompt (IVR). This unit serves to collect information from a subscriber by outputting of voice messages which
5 can be answered by the subscriber by operating keys or by predetermined spoken words.

The identification of the subscriber has been effected according to the Mobile Station Integrated Services
10 Digital Network Number (MSISDN). The MSISDN is a permanent subscriber data stored in a Service Management Point (SMP).

Especially in such a network including IN services it is
15 necessary to grant different access admissions to respective subscribers. That is, if a subscriber to IN services is given access to the SMAP over the network, he must be provided with a user identification (ID) and a password or some other kind of credential.
20

It is important to protect the service management by a password or the like since it has to be avoided that other parties than the subscriber can get access to secret data such as a phone bill or the like.
25 Furthermore, the service provider should be enabled to prove that the subscriber can only get access to those services for which he has paid for.

Heretofore, the password which has been assigned to the
30 corresponding subscriber has been sent to the subscriber by using paper mail, for example. This involves a lot of work for the staff of a service provider and/or network operator. Thus, it is very expensive to grant a huge number of passwords for a huge number of subscribers.

- 3 -

Therefore, the way of granting a password (or any other form or credential) according to this prior art as described above is complicated, troublesome and costly.

5

SUMMARY OF THE INVENTION

Thus, the object underlying the invention is to eliminate the above drawbacks of the prior art and to provide a
10 method and an apparatus by which a password or different kinds of security code can be supplied to a subscriber in an uncomplicated manner.

This object is solved by a services management method for
15 managing subscriber services, comprising the steps of assigning an access code to a subscriber, encapsulating the access code into a data message, and transmitting the data message via a corresponding data channel of the network to a terminal of the subscriber.

20

Furthermore, the above object is solved by a services management device for managing subscriber services, comprising an access granting means for assigning an access code to a subscriber, a message generating means
25 for encapsulating the access code into a data message, and a transmitting means for transmitting the data message via a corresponding data channel of the network to a terminal of the subscriber.

30 By the above method, the delivery of an access code such as a password is performed by using an existing kind of data messages, for example, a Short Message Service (SMS) message. The method according to the invention can easily be performed in a Service Management Access Point (SMAP)
35 without involving the staff of a IN service provider.

- 4 -

Thus, an uncomplicated handling regarding the provision of passwords to the subscribers is possible. Furthermore, it is also very easy for the subscriber to use his password
5 since it is sent to the mobile station which he uses for accessing the corresponding Intelligent Network.

Moreover, it is very easy to regularly change the password in order to provide a higher security when
10 accessing the network. This is because new passwords can easily be sent by using the data channel. Sending passwords via paper mail during short intervals would be very complicated and troublesome for the staff of the IN services provider and also for the user.
15 Further advantageous developments are defined in the dependent claims.

20 BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings in which:

25 Fig. 1 shows a structure of a network including Intelligent Network (IN) services according to an embodiment of the invention, and

Fig. 2 a flowchart of a process for delivering a password
30 to a subscriber according to the embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following, a preferred embodiment of the invention is described in more detail with reference to the
5 accompanying drawings.

Fig. 1 shows a structure of a general network system in which IN (Intelligent Network) services are provided. A user terminal which can be a mobile station (MS), for
10 example, is denoted with reference numeral 1. This mobile station is connected via a mobile network 2 with a Mobile Services Switching Center (MSC) 3.

The MSC 3 comprises a Service Switching Point (SSP) 31 which implements a service switching function and which also provides an interface between a Services Control Point (SCP) 4 and the MSC 3. The SCP 4 serves to control the services requests etc. and is the function in the telecommunications network, which has access to data and
20 logic for controlling processing of a call in order to provide a supplementary service. The SCP 4 is connected with a service management point (SMP) 5 in which IN services offered in the corresponding Intelligent Network are managed. In particular, also subscriber data such as
25 an MSISDN (Mobile Station ISDN Number, i.e., Mobile station Integrated Services Digital Network Number) are stored in the SMP 54.

Reference numeral 6 describes a Service Management Access
30 Point (SMAP) connected to the SMP 5. The SMAP 6 serves to control access from a subscriber to the SMP 5.

Reference numeral 7 denotes a web server of an IN service provider. The web server 7 provides an interface between

- 6 -

the subscriber terminal, i.e., a web browser 9 and the SMAP 6 via the Internet 8.

Reference numeral 10 denotes a Short Messages Service Center (SMSC) which controls the short messages and which provides a connection between the SMAP 6 and the MS 1 via the mobile network 2.

It is to be noted that for simplifying the description, 10 all further elements necessary to establish the connection (e.g., base stations BS and base station controllers BSC) are omitted.

In general, when the subscriber grants access to the 15 basic (call related) IN services, he does not have to provide a password. He is authenticated by the A-number (MSISDN). Only when services (or access to service management) are provided over another network (such as the Internet 8), another way to authenticate the 20 subscriber has to be implemented.

That is, in order to get access to the IN services offered by the SMP to the subscriber via the Internet (by using his web browser 9), the subscriber must know his 25 password and submit his password when requesting an IN service. Thus, initially, a password must be assigned to the subscriber and transmitted to the subscriber.

By using the password, the subscriber can establish a 30 secure connection to the web-server 7 of the service provider. Furthermore, in case the security has been compromised (e.g., the password has become public), a new password can be issued.

- 7 -

It is to be noted that the password is only an example for an access code which is necessary for the subscriber to get access to the IN services. Such an access code can also include only a subscriber ID number or can include
5 an MSISDN number and the password. Furthermore, other forms of credential can be included in the access code.

According to this embodiment, the transmission of the password from the SMAP 6 to the subscriber is effected by
10 using a Short Message Service (SMS).

The Short Message Service (SMS) is a service which is implemented in almost all mobile stations. In general, SMS messages are utilized to communicate text data
15 between a serving Mobile Services Switching Center (MSC) and a mobile station (MS). SMS provides a high degree of privacy compared to, e.g., e-mails. Thus, SMS is an appropriate medium to transmit passwords or the like.
20 Using SMS messages, the serving center or any other connected node can transmit user information to the mobile station and have the mobile station store the received user information. The SMS messages are transmitted via a Short Message Service Center (SMSC).
25 Thus, the connection provided by the SMS is a data channel via which the data messages (SMS messages) containing the password are transmitted.

In the following, the elements necessary for the initial
30 transmission of the password are described in more detail.

The SMAP 6 comprises an assigning means 61 which assigns a password to a subscriber. For example, this can be
35 effected in response to a request for granting a password

- 8 -

from the corresponding subscriber. As an alternative, the passwords for access to service management can also be given in a bulk to the subscribers. However, this can also be effected during predetermined intervals (e.g., 5 once a week) such that the password is changed regularly in order to improve the security of the access of the subscriber.

The assigned password is supplied to a message generator 10 62. This message generator 62 is adapted to encapsulate the password into an SMS message.

The SMS message containing the password is then supplied to a transmitter 63. The transmitter 63 is adapted to 15 transmit SMS messages via the Short Message Service Center (SMSC) 10. The SMSC 10 provides a connection between the SMAP 2 and the mobile station (MS) 1 of the subscriber via the mobile network 2. The MS 1 comprises a detector 11 which is adapted to receive the SMS message.

20 The method for transmitting the password performed in the above described devices is shown in the flowchart of Fig. 2.

25 Steps S1 to S3 are performed on the IN service management side (i.e., in the SMAP 6), whereas steps S4 to S5 are performed on the subscriber side (i.e., in the mobile station MS 1).

30 In step S1, the password is assigned to a subscriber. In step S2, the password is encapsulated in an SMS message. Then, the SMS message is transmitted to the mobile station via an SMS connection (SMS data channel), i.e., via the SMSC 10 and the mobile network 2.

- 9 -

In step S4, the SMS message is received by the mobile station. In step S5, the password is detected in the SMS message and shown on a display of the mobile station.

Preferably, the password should not be automatically

5 displayed but on demand of the subscriber, for example by operating a special key or inputting a special code for reading SMS messages. This measure avoids that other persons than the subscriber can accidentally read the password.

10

The above embodiment has been described such that the password is sent by using an SMS message. As an alternative of this embodiment, the password can also be transmitted by a so-called Unstructured Supplementary

15 Service Data (USSD) message.

In general, using USSD messages, a mobile telecommunication network is able to transparently communicate text data with a mobile station. Hence, the 20 mobile station may receive and display text messages on an attached display unit.

Thus, USSD messages are similar to SMS messages with respect to the capability of sending text data to a 25 subscriber. Hence, also USSD messages can be used to transmit a password to the corresponding subscriber.

In case of using USSD messages instead of SMS messages, the message generator 62 and the transmitter 63 of the 30 SMAP 6 and the SMSC 10 have to be correspondingly modified. In particular, the USSD message has to be transmitted via a USSD data channel.

It is to be noted that the above embodiment has been 35 described with respect to a mobile telecommunication

- 10 -

network (e.g., a GSM network). However, the invention can also be applied to fixed networks as long as the terminals are adapted to receive data messages such as SMS or USSD messages.

5

As described above, by using the method according to the invention, an access code like a password can be transmitted from a Service Management Access Point SMAP 2 to the terminal 4 of a subscriber via a data message such 10 as a Short Message Service SMS message. Thus, a necessary password can easily be supplied to the subscriber without the need of complicated work of a staff of an IN service provider or the like. Furthermore, the method can easily be implemented, since almost all mobile stations support 15 Short Message Service (SMS).

The above description and accompanying drawings only illustrate the present invention by way of example. Thus, the embodiments of the invention may vary within the 20 scope of the attached claims.

ART 34 AMDT

Enclosure of October 5, 2001

PCT Patent Application No.: PCT/EP 99/06176
NOKIA NETWORKS OY
Our ref.: WO 24040

New claims 1 to 12

1. A services management method for managing subscriber services in an Intelligent Network, in which a subscriber or service provider can manage his own services, comprising the steps of:

- 5 assigning (**S1**) an access code to a subscriber by which the subscriber is allowed to get access to services or to service management via another network (**8**);
encapsulating (**S2**) said access code into a data message; and
10 transmitting (**S3**) said data message via a corresponding data channel of said network to a terminal (**1**) of said subscriber.

2. The services management method according to claim 1,
15 wherein said access code comprises a password.

3. The services management method according to claim 1 or 2, wherein said access code comprises a subscriber identification number.

20
4. The services management method according to claim 1, wherein said data message is a Short Message Service (SMS) message.

ART 34 AMDT

- 2/3 -

5. The services management method according to claim 1, wherein said data message is an Unstructured Supplementary Service Data (USSD) message.

5 6. The services management method according to any one of the previous claims, further comprising the step of detecting (S5) said access code in said terminal of said subscriber.

10 7. A services management device for managing subscriber services in an Intelligent Network in which a subscriber or service provider can manage his own services, comprising:

15 an access granting means (61) for assigning an access code to a subscriber by which the subscriber is allowed to get access to services or to service management via another network (8);

20 a message generating means (62) for encapsulating said access code into a data message; and

20 a transmitting means (63) for transmitting said data message via a corresponding data channel of said network to a terminal (1) of said subscriber.

8. The services management device according to claim 7, 25 wherein said access code comprises a password.

9. The services management method according to claim 7 or 8, wherein said access code comprises a subscriber identification number.

30 10. The services management device according to claim 7, wherein said data message is a Short Message Service (SMS) message.

- 3/3 -

11. The services management device according to claim 7,
wherein said data message is an Unstructured
Supplementary Service Data (USSD) message.

5 12. A subscriber terminal which is adapted to receive
data messages transmitted by a services management device
according to any one of the claims 8 to 11, comprising a
detecting means (11) for detecting said access code.

10

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/15462 A1

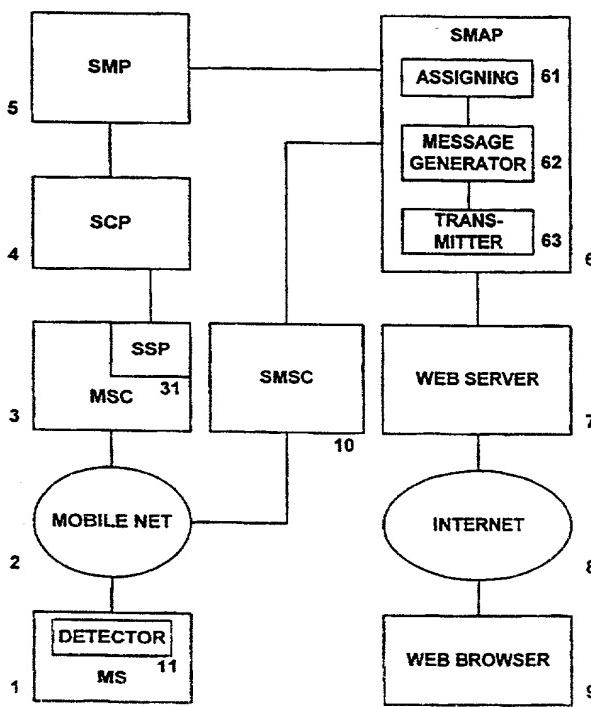
- (51) International Patent Classification⁷: H04Q 3/00, H04L 29/06, H04Q 7/22
- (21) International Application Number: PCT/EP99/06176
- (22) International Filing Date: 23 August 1999 (23.08.1999)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): NOKIA NETWORKS OY [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): ANDERSEN, Michael, Tulinius [DK/DK]; Huldbergs Allé 32, DK-2800 Lyngby (DK).
- (74) Agents: PELLMANN, Hans-Bernd et al.; Tiedtke-Bühling-Kinne et al., Bavariaring 4, D-80336 München (DE).
- (81) Designated States (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— With international search report.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

- (54) Title: SENDING INITIAL PASSWORD THROUGH AN SMS



(57) Abstract: The present invention discloses a services management method for managing subscriber services, comprising the steps of assigning an access code to a subscriber, encapsulating said access code into a data message, and transmitting said data message via a corresponding data channel of said network to a terminal (1) of said subscriber. By using this method, an access code like a password can be sent from a Service Management Access Point (SMAP) (6) to the terminal (1) of a subscriber via a data message such as a Short Message Service (SMS) message.

WO 01/15462 A1

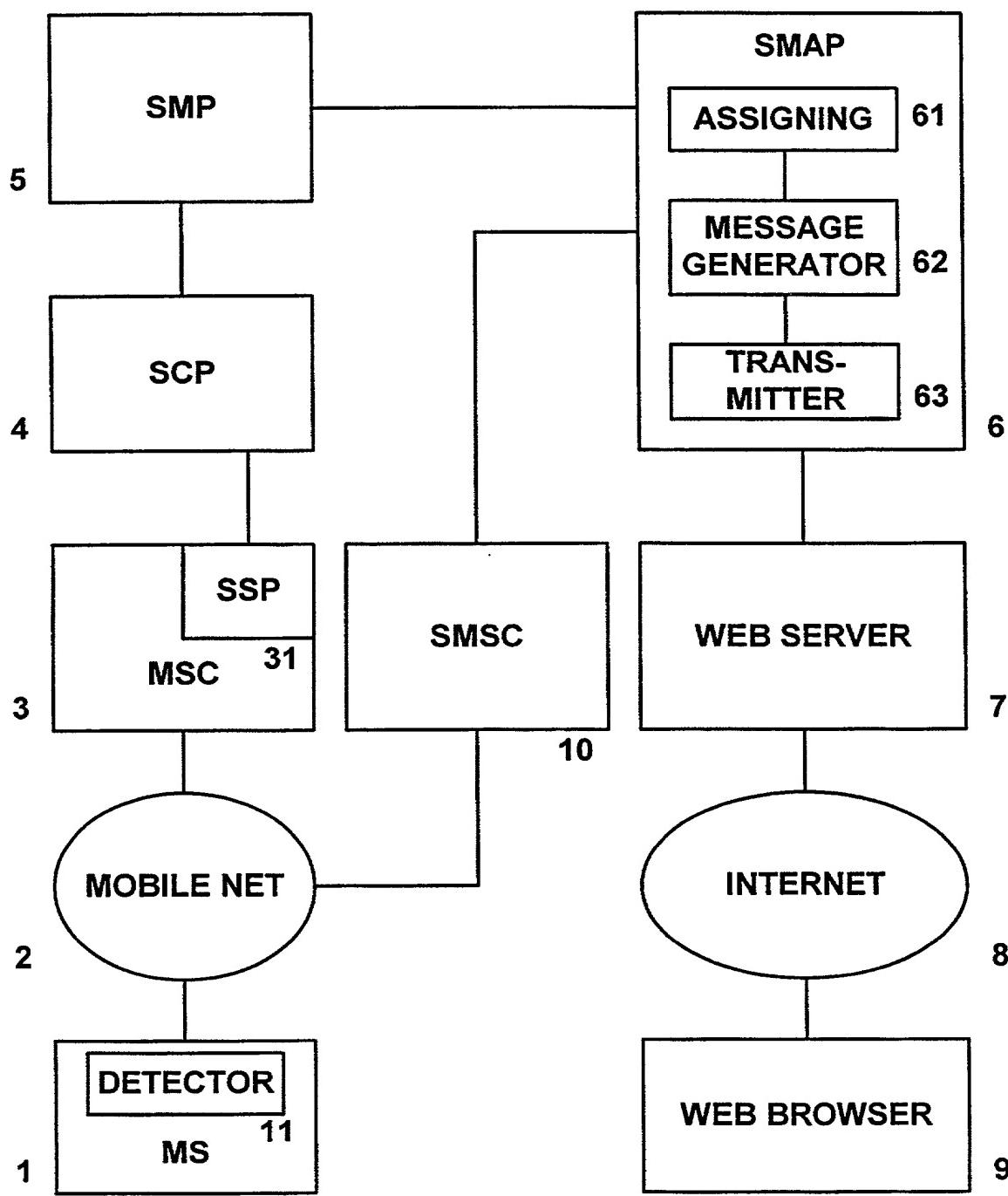


FIG. 1

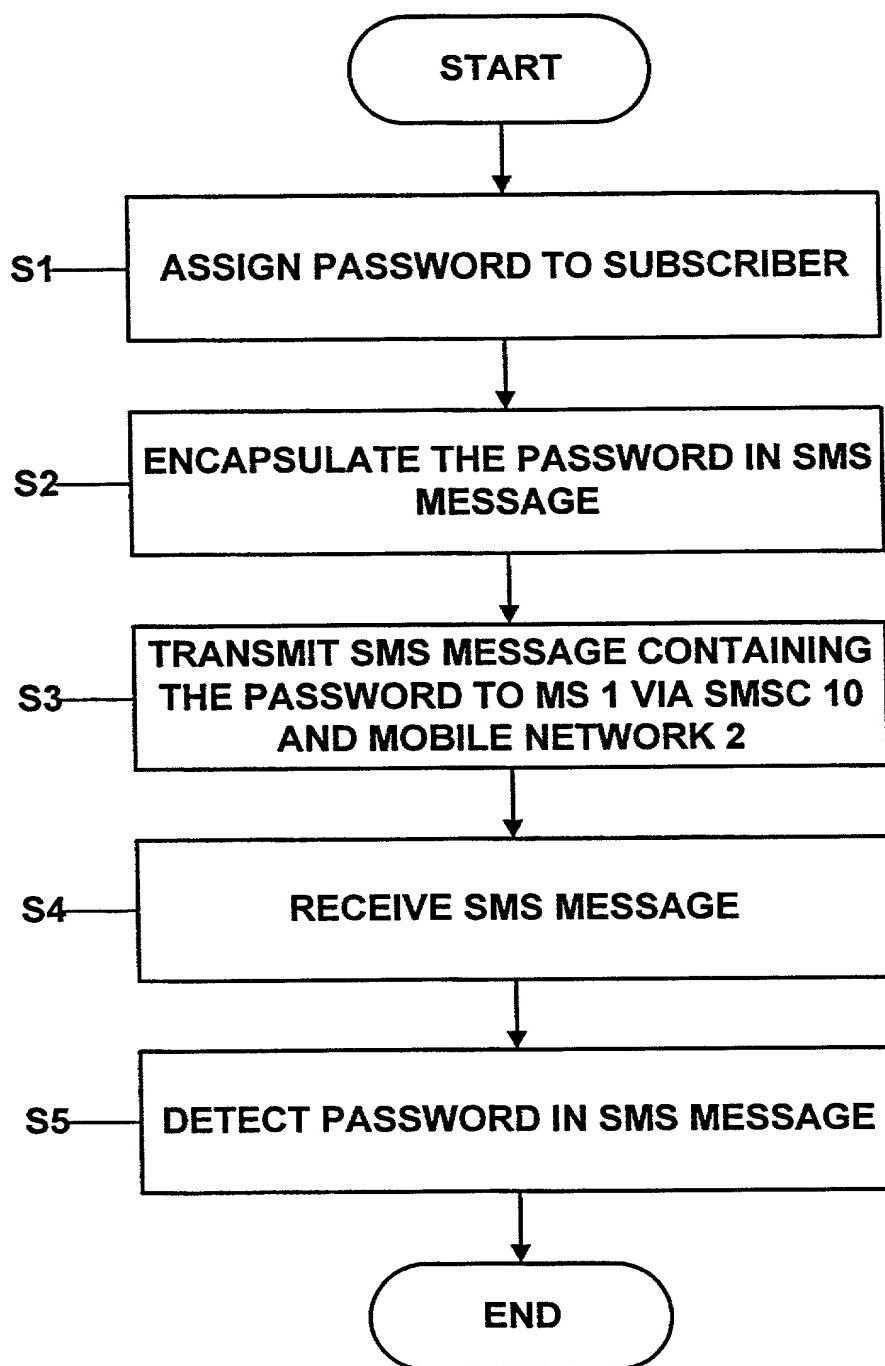


FIG. 2

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY
Includes Reference to PCT International Applications

Attorney's Docket
No. 4925-206pus

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SENDING INITIAL PASSWORD THROUGH AN SMS

the specification of which (check only one item below)

- is attached hereto
 was filed as United States application

Serial No. __

on __

and was amended

on __ (if applicable).

[x] was filed as PCT international application

Number PCT/EP99/06176

on 23 August 1999

and was amended under PCT Article 19

on __ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of the application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

PRIOR FOREIGN/PCT APPLICATIONS AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

Country (if PCT, indicate "PCT")	Application Number	Date of Filing (day, month, year)	Priority Claimed Under 35 U.S.C. 119	
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
PCT	PCT/EP99/06176	23 August 1999	<input checked="" type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO

Combined Declaration for Patent Application and Power of Attorney (Continued)
(Includes Reference to PCT International Applications)

Attorney's Docket No.
4925-206pus

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S. APPLICATIONS		STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S. SERIAL NUMBERS ASSIGNED (if any)		
PCT/EP99/06176	23 August 1999		X	

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (*List name and registration number*)

19
MYRON COHEN, Reg. No. 17,358; THOMAS C. PONTANI, Reg. No. 29,763; LANCE J. LIEBERMAN, Reg. No. 28,437; MARTIN B. PAVANE, Reg. No. 28,337; MICHAEL C. STUART, Reg. No. 35,698; KLAUS P. STOFFEL, Reg. No. 31,668; EDWARD WEISZ, Reg. No. 37,257; VINCENT M. FAZZARI, Reg. No. 26,879; JULIA S. KIM, Reg. No. 36,567; ALFRED FROEBRICH, Reg. No. 38,887; ALFRED H. HEMINGWAY, JR., Reg. No. 26,736; KENT H. CHENG, Reg. No. 33,849; YUNLING REN, Reg. No. 47,019; ROGER S. THOMPSON, Reg. No. 29,594; BRICE FALLER, Reg. No. 29,532; DAVID J. ROSENBLUM, Reg. No. 37,709; TONY CHEN, Reg. No. 44,607; ELI WEISS, Reg. No. 17,765; TEODOR J. HOLMBERG, Reg. No. 50,140.

Send correspondence to: Michael C. Stuart Reg. No. 35,698 Cohen, Pontani, Lieberman & Pavane 551 Fifth Avenue, Suite 1210 New York, New York 10176	Direct Telephone calls to: (name and telephone number) Michael C. Stuart (212) 687-2770
---	--

2 0 1	FULL NAME OF INVENTOR <i>DK</i>	FAMILY NAME <u>ANDERSEN</u>	FIRST GIVEN NAME <u>Michael</u>	SECOND GIVEN NAME <u>T.</u>
	RESIDENCE, CITIZENSHIP	CITY <u>Lyngby</u>	STATE OR FOREIGN COUNTRY <u>Denmark</u>	COUNTRY OF CITIZENSHIP <u>Denmark</u>
POST OFFICE ADDRESS	POST OFFICE ADDRESS <u>Huldbergs Allé 32</u>	CITY <u>Denmark</u>	STATE & ZIP CODE/COUNTRY <u>DK-2800</u>	
2 0 2	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE, CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

Combined Declaration for Patent Application and Power of Attorney (Continued)
 (Includes Reference to PCT International Applications)

Attorney's Docket No.
4925-206pus

2 0 3	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE, CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201 <i>X Michael Anderson</i>	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
DATE <i>X 04/18/2002</i>	DATE	DATE